CalCloud IaaS

Service Availability Plan

Office of Technology Services

Version 1.7

December 2015

1 Executive Summary

The purpose of this availability plan is to document and communicate the existing and future availability requirements for CalCloud services offered by the California Department of Technology (CDT), which can be provided effectively to meet the Vital Business Function (VBF) requirements of its Customers.

1.1 Description of Service Area

CalCloud Infrastructure as a Service (CalCloud IaaS) provides Customers with a private cloud located at the CDT data centers. Using a self-service portal, CalCloud IaaS customers have on-demand access to a shared pool of computing resources that can be rapidly provisioned and released as virtual servers on a pay-as-you-go basis. Additional add-on options such as increased Storage, RAM, Disaster Recovery, and Backups are available during and after provisioning. Network firewall access between provisioned servers and any external access is also requested by customers using the self-service portal.

2 Introduction

2.1 Purpose

This plan is intended to ensure that existing objectives for CalCloud services can be effectively provided and meet customer VBF requirements.

2.2 Objectives

The following objectives shall be met within this plan:

i) Define availability level requirements for CalCloud IaaS
ii) Document the activities of monitoring and reporting service availability
iii) Inform customers as to the availability of current CalCloud IaaS services

2.3 Scope

This plan applies to the following IT service: CalCloud IaaS.

2.3.1 Demarcation of Services

The boundaries of the CalCloud Service Availability Plan are restricted to the tenant virtual environments supporting infrastructure and network services out to the CalCloud Edge firewalls, which includes the CalCloud Disaster Recovery supporting infrastructure at the Vacaville Data Center. CSGNET/CGEN network services, as well as other CDT IT services, are beyond the scope of this agreement.

3 Plan Content

3.1 Background

Availability has an immediate impact on the way the business and the users perceive the quality of the services they receive. This plan addresses the service availability objectives.

3.2 Service Operations

The CalCloud service is supported in the same manner as any other CDT service. As such, all incidents, changes, service requests and related work orders are logged and tracked in the Enterprise IT Service Management System (currently BMC's Remedy as of the date of this Plan).

3.2.1 Service Desk

The CDT Service Desk is available twenty-four hours a day, seven days a week, and 365 days a year (24x7x365) to receive and respond to customer communications. Any customer requiring service assistance can contact the Service Desk at (916) 464-4311.

CDT Service Desk staff will:

i) Serve as the initial point-of-contact for service-related incidents
ii) Log service-related incidents and assign the incident to the CalCloud service team
iii) Communicate service interruption, degradations, and restorations to impacted customer(s).

Additionally, customers can open an incident ticket directly via CDT's web-based Incident reporting system (Remedy), or by accessing Remedy via the CalCloud Portal to open the incident.

3.2.2 Technical Support Resources

Standard technical support resources are available during primary business hours from 8:00 a.m. to 5:00 p.m. Pacific Standard Time, Monday through Friday, excluding holidays and State non-work days. Standard technical support resource availability is not guaranteed outside of primary business hours.

24x7x365 support is available for Incident tickets marked as either "critical" or "high" and will be addressed by the CalCloud Service Provider (CSP) within the time frames defined below in *Section 3.2.4 Incident Management Table 3.*

3.2.3 Maintenance Schedule

Planned maintenance for CalCloud IaaS that may have an impact on customer services will be scheduled during the planned maintenance windows. Maintenance follows the CDT Change Management and notification process.

3.2.4 Service Incident Management

The CDT Service Desk is the initial point-of-contact for all CalCloud customers to report service incidents. The CDT Service Desk will record service incidents for the CalCloud Service on a 24x7x365 basis, and assign the incidents to the CalCloud service team. The CDT Service Desk will acknowledge each reported service incident by providing the customer with a unique service incident reference number (INC #) when a service incident is reported by either telephone or email. The CDT Service Desk will provide service incident resolution progress updates via email to all known impacted customers, if the incident is deemed to be a Major Incident. If the incident is not a Major Incident, the CalCloud service team will provide updates to the impacted customers.

Upon receipt, service incidents will be assessed and classified using the criteria illustrated in Table 2: Service Incident Classification, shown below.

Service incident resolution efforts by CalCloud technical service groups will occur based on the service incident priority. With the agreement of the customer, the priority of a service incident may be lowered before a service incident is resolved. This typically occurs when circumvention (work around) is available.

Table 2 Service Incident Classification depicts how CDT and the CalCloud Service Provider will apply technical team efforts to resolve service incidents based on the service incident priority.

Table 2: Service Incident Classification

PRIORITY	IMPACT	RESOLUTION APPROACH
Critical	**Extensive/Widespread**	Major system or virtual network outage, multiple sites or organizations down.
High	**Significant/Large**	A single site or organization is down, or significantly degraded.
Medium	**Moderate/Limited**	A single user is down, or services degraded, but operational.
Low	**Minor/Localized**	Minimal impact to services, a CalCloud Consumer question or request.

When the service incident is resolved, the CalCloud service team will contact the customer to report the repair is complete and will request the customer validate the service restoration was successful. The status of a service incident is then changed to closed, but only after the customer agrees that the repair was successful or if after several (3 or more) documented, unsuccessful attempts to contact the customer for verification.

Table 3: Service Incident Resolution Service Objective, shown below, lists the resolution timeframe service objective.

PRIORITY	RESPONSE TIME		ESCALATION INTERVALS
		Assigned Status	**Pending or Resolved Status**

Critical	≤ 15 minutes	15 Minutes	4 Hours
High	≤ 30 minutes	30 minutes	8 hours
Medium	≤ 2 hours	2 hours	---
Low	≤ 4 hours	4 hours	---

3.2.5 Change Management

All CDT CalCloud changes comply with CDT's Change Management Process and Policy. Any change that may impact the customer will result in a CDT Service Desk Bulletin being sent to all potentially impacted customers. Tenant application changes do not go through the CDT's Change Management Process and will follow their own department practices.

3.3 Service Objectives

The Service Level Objectives (SLOs) provided below do not include planned/scheduled downtime or maintenance:

1. Backup Tier 1 Recovery Point Objective (RPO) is <1 hour.
2. Backup Tier 2 RPO is <= 24 hours.
3. Infrastructure Disaster Recovery (IDR) Recovery Time Objective (RTO) for Tier 1 is <1 hour.
4. IDR RTO for Tier 2 is <96 hours.
5. Backup/Restore Availability for "Critical" Incidents is <2 hours.
6. Backup/Restore Availability for "High" Incidents is 8 hours.
7. CalCloud Service Uptime 99.9% per a month.
8. CalCloud Service Monitoring cannot exceed 1 hour of cumulative outages during a calendar month.
9. CalCloud Storage uptime is 99.9% per a month.
10. OS Security Patching updates applied within 30 days of release and validation by OTech/CSP.

3.4 Exclusions

The CalCloud Service Objective and any applicable Service Levels do not apply to any performance or availability interruptions or degradations in the following:

i. Any factors outside CDT's or the CSP's reasonable control;
ii. Caused by adverse actions or inactions of the customer, their agents, or third parties;
iii. During scheduled downtime and maintenance.

3.5 CalCloud Infrastructure Disaster Recovery

The disaster recovery component within CalCloud is used to plan, test, and execute emergency failover of critical data center services between the Gold Camp and Vacaville sites. Emergency failover begins at the time CDT Executive Management declares an emergency at the Gold Camp Data Center. IDR services cannot be implemented separately for tenants. The failover of services to Vacaville will include all IDR tenant servers subscribing to the service.

There are two tiers for the CalCloud IDR service.

3.5.1 Tier 1

This tier of Infrastructure Disaster Recovery (IDR) has a 1-hour RPO and a 1-hour RTO. The 1-hour RPO means that the re-constituted environment will be restored with no more than 1 hour's loss of data and state (i.e., it will reflect the source system as it existed at some point in time in the hour preceding the failure). The 1-hour RTO means that the re-constituted environment will be available to tenants no more than 1 hour following the declaration of the disaster by CDT (not the actual time of the disaster event).

3.5.2 Tier 2

This IDR tier has a 24-hour RPO and 96-hour RTO. Otherwise, the same conditions also apply to Tier 2 objectives as to Tier 1 objectives.

3.6 Security

The CalCloud IaaS is secured based on industry best practices and has been implemented conforming to National Institute of Standards and Technologies (NIST) controls and processes as defined by the Federal Risk and Authorization Management Program (FedRAMP). This security framework focuses on securing the infrastructure elements upon which tenant environments are created.

While some of the security monitoring and processes apply to tenant environments (e.g. perimeter Intrusion Detection monitoring inspects packets to/from both the infrastructure and tenant spaces), the securing of the actual tenant environment is the responsibility of the customer (e.g. OS, database services, middleware services, application services, virtual appliances…).

Data-at-Rest and Data-in-Transit encryption services are available in CalCloud IaaS, however, these services are optional and are not implemented by default. In regard to these services, the CalCloud Service staff can be contacted for further information. Additionally, virus protection and OS patching management services are optionally available as well. OS patching will occur within 30 days of release and is conducted on a monthly basis.

Should an anomalous security event be detected within the CalCloud environment, impacted tenants will be notified in a timely manner. Depending on the nature of the security event, the CalCloud Service team and the OTech incident response team will coordinate with those tenants as appropriate to address the specifics of that event. The specifics of that coordinated effort (e.g. resources, staffing, shared data/information…) will be dictated by the nature of the event in question.

CalCloud provides security safeguards that adhere to the operational and compliance requirements of:

I. The California Information Practices Act (Civil Code Sections 1798.3 et seq.);

II. Security provisions of the California State Administrative Manual (Chapters 5100 and 5300) and the California Statewide Information Management Manual (Sections 58C, 58D, 66B, 5305A, 5310A and B, 5325A and B, 5330A, B and C, 5340A, B and C, 5360B);

III. Privacy provisions of the Federal Privacy Act of 1974;

IV. Federal Risk and Authorization Management Program (FedRAMP);

V. Based upon the State's classification of the Data pursuant to SAM 5305.5:

   a. Relevant security provisions of the Internal Revenue Service (IRS) Publication 1075, including the requirement that Data not traverse networks located outside of the United States;

   b. Relevant security provisions of the Social Security Administration (SSA) document electronic information exchange security requirement and procedures for state and local agencies exchanging electronic Information with the SSA;

   c. Relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines and;

   d. Relevant security provisions of the Health Information Portability and Accountability Act (HIPAA) Security Rule and all modifications/extensions